Cybersecurity Maturity Model Certification (CMMC)

What it means for your business and how to tackle it, step-by-step.

CLARE COMPUTER SOLUTIONS

What is CMMC?

The Cybersecurity Maturity Model Certification (CMMC) was introduced by the US Department of Defense (DoD) on January 31, 2020. The CMMC is a new unified standard that aims to implement cybersecurity for over 300,000 companies in the defense industrial base (DIB) supply chain.

Prior to the introduction of CMMC, defense contractors were responsible for implementing, monitoring, and certifying the security of their own IT systems and any sensitive information transmitted by or stored on these systems. With the rollout of CMMC, contractors must now work with third-party auditors to assess and verify their compliance with CMMC practices.

The CMMC model contains five levels of cybersecurity maturity (basic to advanced/progressive) with each level consisting of a different set of processes and practices.

Key Facts:

- **Failure to meet the required CMMC maturity level negates your chances at landing government contracts.**
- **Right now, around 300,000 vendors must comply with CMMC to continue business. The DoD estimates that only 10% of them meet the standard, as released, on January 31, 2020.**
- **The DoD plans to release around 20 RFPs this year that will require CMMC when the contract is awarded.**
- **By FY26, all new DOD contracts will contain CMMC requirements. All DoD contractors should already be at Level 1 as that parallels some existing requirements. Level 3 is going to be the level that most contractors need to achieve to be relevant.**
- **Things have changed some: under the new requirements, you must demonstrate that you are certified prior to the final award. Previous standards allowed you to identify the areas of needed improvement and put them on a Plan of Action and Milestones (POAM) to address later.**

Where to Start: A Step-by-Step Plan

Meeting the requirements of CMMC requires integrating multiple solutions. Depending on the extent of your security defense infrastructure, CMMC compliance may be a significant undertaking and expense to consider. Here's how to tackle it:

1

Make sure you have the right people involved. CMMC and any unintended non-compliance is a risk factor for your company, so you'll need high-level business owners involved in this process in addition to technology owners—particularly those who are responsible for business risk.

2

Get an assessment. The time is yesterday! A CMMC assessment shows your performance against the standard and the gaps you're required to fill. Before you ask: yes, there is a provision for self-audit if you're up to the task; but we can facilitate and speed up this complicated process substantially.

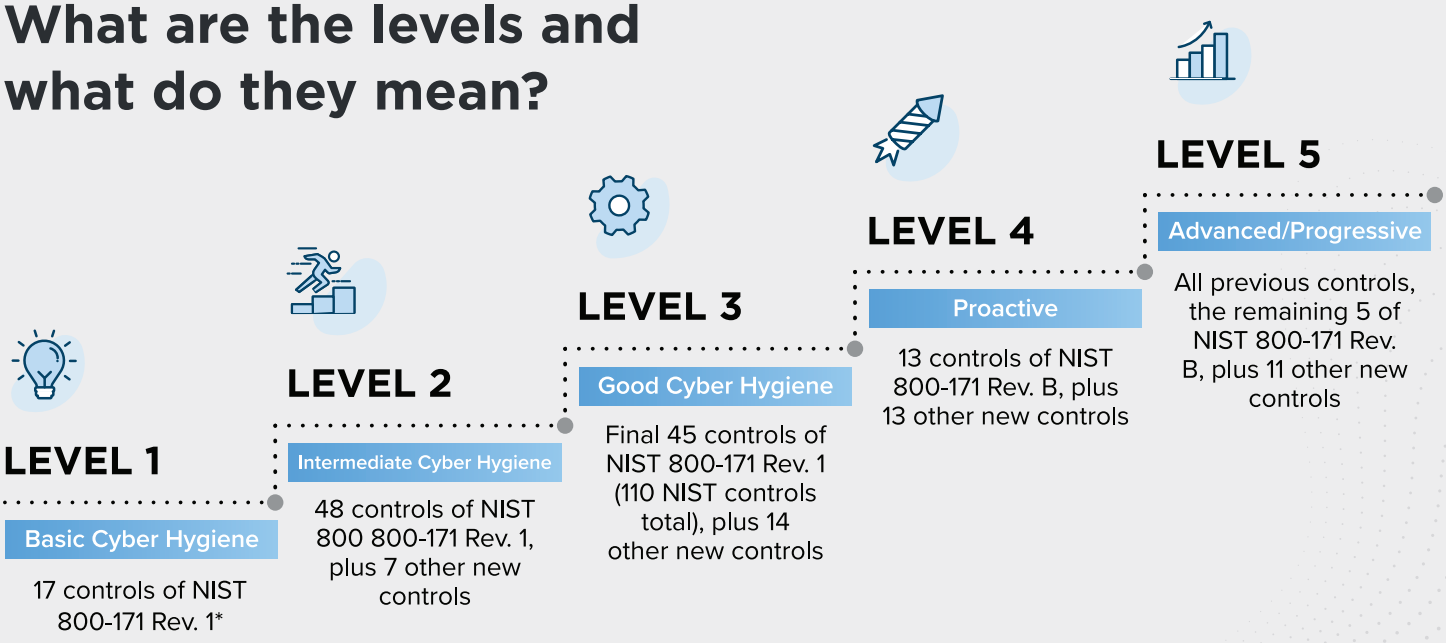
3

Weigh your options. In the end, complying with CMMC may cost more than your DoD revenue stream. You may want to consider selling that IP and the associated manufacturing processes to another larger, already CMMC certified, company rather than take on that compliance expense.

4

Build a plan of action. If you plan to move forward, work with us to decide what gaps to fill first, then we can build a plan together. With the proper partners in the right places at the right time, you can be well on your way to CMMC compliance.

What are the levels and what do they mean?



*National Institute of Standards and Technology (NIST)

Meeting the requirements of CMMC requires integrating multiple solutions. Depending on the extent of your security defense infrastructure, CMMC compliance may be a significant undertaking and expense to consider. **Let's tackle this together and keep your DoD business going strong.**

Clare Computer Solutions
12657 Alcosta Blvd. Suite 160 San Ramon, California, 94583

(925)277-0690 info@clarecomputer.com www.clarecomputer.com